Configurer son interface

(Redirigé depuis Configurer son interface)

Sommaire

1 Configurer son interface
1.1 Les divers modes
1.1.1 Mode Master/AP
1.1.2 Mode Managed
1.1.3 Mode Monitoring / Promiscuous
1.1.4 Mode Ad-hoc
1.1.5 Mode Repeater
1.2 Configuration avec iwconfig et ifconfig
1.3 Configuration avec airmon-ng
1.4 Se connecter à un réseau wifi
1.4.1 Avec le WPA
1.4.2 Avec le WEP
2 Cas particulier de carte wifi
2.1 IPW2200
3 Cas particulier de carte ethernet
3.1 Intel PRO/100 & PRO/1000
4 Cas particulier de Dongle USB
4.1 Drivers RTL8187
4.1.1 [BACTRACK 5R1]
4.2 Drivers RT 73 - Linksys WUSB54GC
4.2.1 [BACTRACK 3 FINAL]
4.2.2 [BACTRACK 3beta]
4.2.3 [BACKTRACK V2]
5 Problèmes
5.1 Channel Négatif

Configurer son interface

Cette page rassemble des informations sur la configuration de carte réseau.

Les divers modes

Une carte réseau dispose de plusieurs modes (monitoring, ad-hoc, ...) selon son cas d'utilisation dans un réseau. Ici nous vous proposons une liste de commandes pour mettre votre carte dans ces modes.

Mode Master/AP

On est en mode "Access Point", autrement dit, il représente le passage vers le réseau éthernet, on peut l'appeler maitre ou père du réseau.

Mode Managed

Ici, on représente qu'un client du réseau sans fil, on peut l'appeler esclave ou fils du réseau. C'est le mode utilisé le plus courant chez les utilisateurs.

Mode Monitoring / Promiscuous

Le mode monitoring (ou "surveillance") est une notion appartenant aux réseaux sans fil, où nous ne sommes pas associé/connecté aux réseaux écoutés. Le mode promiscuous, est une notion utilisée dans un contexte d'association avec le réseau, c'est une option que doit disposer de sa carte réseau. A la base elles ignorent les paquets qui ne nous sont pas destinés, or en activant ce mode, nous pourrons accéder à tous les paquets qui transitent par notre machine.

Mode Ad-hoc

Le mode client à client, vous pouvez constituer ainsi un réseau sans AP... Si les ordinateurs A, B et C ont constitué un même réseau sans fil ad-hoc nommé NET-ABC, si C est hors de portée de A, et B entre les deux, alors A et C ne pourront pas communiquer, seul B le pourra avec les deux. B ne jouera pas le rôle du relayeur pour lier A et C.

Mode Repeater

Vous êtes un relayeur de signal, pour étendre la portée de l'AP.

Configuration avec iwconfig et ifconfig

Nous commençons par définir notre interface wifi. La commande “iwconfig” permet cela.

```
bt ~ # iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

rausb0    RT73 WLAN
           Link Quality:0  Signal level:0  Noise level:113
           Rx invalid nwid:0  invalid crypt:0  invalid misc:0

bt ~ #
```

Nous activons cette interface avec la commande ifconfig.

```
bt ~ # ifconfig rausb0 up
```

Nous positionnons notre carte en mode “Ecoute”. Cela nous permettra d’injecter des paquets et d’écouter sur les paquets transitant sur le réseau.

```
bt ~ # iwconfig rausb0 mode Monitor
```

Configuration avec airmon-ng

Airmon-ng est un utilitaire, qui sert uniquement à activer/désactiver votre carte wifi du mode monitoring. Il peut se substituer à iwconfig.

- Usage :

```
airmon-ng <start|stop> <interface> [channel]
```

```
bt ~ # airmon-ng start rausb0 6
```

Ici, l'interface rausb0 est réglée en mode Monitor sur le channel 6.

Se connecter à un réseau wifi

Vous devrez avoir préalablement configuré votre station wifi avec le cryptage adéquat, nous vous conseillons le cryptage WPA. (Se reporter à la documentation de votre fournisseur d'accés internet) Les exemples ci-dessous servent uniquement à votre client.

Avec le WPA

Créez un fichier wpa_supplicant.conf : (* si wpa_supplicant ne fonctionne pas cf quelques lignes plus bas)

```
nano wpa_supplicant.conf
```

Dans ce fichier inscrire :

```
network={
ssid="NOM_DU_RESEAU"
key_mgmt=WPA-PSK
proto=WPA
pairwise=TKIP
group=TKIP
psk="Phrase WPA"
}
```

Activez ensuite l'interface Wifi, eth0 sera ici utilisé.

```
ifconfig eth0 up
```

Lancez wpa_supplicant :

```
wpa_supplicant -i eth0 -c wpa_supplicant.conf
```

Configurer l'adresse IP et le masque de sous-réseau de l'interface (à adapter en fonction de votre réseau) :

```
ifconfig eth0 inet 192.168.1.123 netmask 255.255.255.0
```

Configurez les routes (à adapter en fonction de votre réseau) :

```
route add default gw 192.168.1.1
```

Configurez les DNS :

```
echo nameserver 192.168.1.1 > /etc/resolv.conf
```

Testez la configuration :

```
ping google.fr
```

- Si wpa_supplicant ne fonctionne pas voici une autre methode pour se connecter en wpa

dans cet exemple ra0 correspond à notre carte wifi, remplacer le nom de la carte avec la votre

(pour connaitre le nom de votre carte wifi tapez dans la console iwconfig).

Donc pour se connecter avec une clé wpa voici le code console à utiliser :

```
ifconfig ra0 up && iwconfig ra0 channel 11 && iwconfig ra0 essid votre_essid_ici && iwpriv ra0 set AuthMode=WPAPSK
&& iwpriv ra0 set EncrypType=TKIP && iwpriv ra0 set WPAPSK="votre_cle_ici"
```

(ensuite tapez entrée puis activez la connection avec dhcpcd toujours avec la console)

dhcpcd ra0

Voila essayez d'ouvrir une page web par exemple google avec firefox.

Avec le WEP

Pour configurer votre interface avec la sécurité WEP. À proscrire.

```
root~# iwconfig rausb0 essid TON_ESSID
root~# iwconfig rausb0 channel TON_CHANNEL
root~# iwconfig rausb0 key TA_CLEF_EN_HEXA
     ou root~# iwconfig rausb0 key s:TA_CLEF_EN_ASCII
root~# ifconfig rausb0 up
root~# dhcpcd rausb0
```

Cas particulier de carte wifi

IPW2200

Driver : IPW2200 (Avec patch d'injection). Démarrage sur le Live CD et installation sur le disque. Détéction et installation des drivers patchés. L'injection ne peut être utilisée pour la déauthentification de client. Uniquement les options : "– interactive, –arpreplay et –chopchop" d'aireplay-ng fonctionnent. C'est dû a une limitation de l'ipw2200.

Activer l'interface rtap0 avec les commandes suivantes pour rendre l'injection possible :

```
- rmmod ipw2200
- modprobe ipw2200 rtap_iface=1
- ifconfig eth1 up
- ifconfig rtap0 up
```

L'injection fonctionne en utilisant : "-i rtap0 eth1". Cela permet d'écouter en même temps avec airodump-ng sur l'interface rtap0.

Exemple d'injection d'arp:

```
- aireplay-ng --arpreplay -b 00:00:00:00:00:00 -h 11:11:11:11:11:11 -i rtap0 eth1
```

Cas particulier de carte ethernet

Intel PRO/100 & PRO/1000

Chargez le module correspondant à votre carte:

```
-modprobe e100 #si votre carte est une PRO/100
-modprobe e1000 #si votre carte est une PRO/1000
```

Cherchez votre interface reseau (ethernet) avec:

```
-ifconfig -a
```

Dans mon cas l'interface est eth1.

Activez eth1:

```
-ifconfig eth1 up
```

```
Si vous utilisez un routeur, activez le dhcp puis attribuez une adresse ip à votre carte réseau avec dhcpcd:
```

```
-dhcpcd -d eth1
```

Cas particulier de Dongle USB

Drivers RTL8187

[BACTRACK 5R1]

(testé avec Awus06H) Si vous avez un asus, et que l'interface de votre carte wifi USB ne remonte pas au airmon-ng, essayez ceci:

rmmod asus_nb_wmi

rmmod asus_wmi

ifconfig wlan1 up

Si ce n'est pas suffisant, faire rmmod de rfkill, cfg80211,iwlagn,mac80211,rtl8187 puis modprobe rtl8187 ifconfig wlan1 up

Drivers RT 73 - Linksys WUSB54GC

[BACTRACK 3 FINAL]

Downgrader le drivers RT73 de la version 3 à la version 2. (pour le version live cd il faut aussi les sources du kernel)

```
wget http://homepages.tu-darmstadt.de/~p_larbig/wlan/rt73-k2wrlz-2.0.0.tar.bz2
ifconfig rausb0 down
airdriver-ng remove 31
tar -xvjf rt73-k2wrlz-2.0.0.tar.bz2
cd rt73-k2wrlz-2.0.0
cd Module
make
make install
modprobe rt73
ifconfig rausb0 up
```

[BACTRACK 3beta]

fonctionne out of the box

Quelque probleme sur les box wanadoo, numericable ...

[BACKTRACK V2]

La carte est reconnue sans problème par Backtrack mais si vous voulez profiter pleinement de ses capacités avec aircrack-ng, il vous faudra apporter les modifications suivantes :

1) Downloader le module rt73-ASPJ-1.1.0

```
http://www.backtrack-fr.net/Downloads/Drivers/rt73-ASPJ-1.1.0.tgz
http://www.backtrack-fr.net/Downloads/Drivers/rt73-ASPJ-1.1.0.lzm
ftp://ftp.berlios.de/pub/svair/rt73-ASPJ-1.1.0.tgz
```

2) Installer le module rt73-ASPJ-1.1.0

Installer directemement le module lzm ou alors taper la commande suivante : tgz2lzm

```
/usr/bin/tgz2lzm rt73-ASPJ-1.1.0.tgz rt73-ASPJ-1.1.0.lzm
```

qui devrait vous donner ceci :

```
bt Desktop # /usr/bin/tgz2lzm rt73-ASPJ-1.1.0.tgz rt73-ASPJ-1.1.0.lzm
Installing package rt73-ASPJ-1.1.0...
PACKAGE DESCRIPTION:
Executing install script for rt73-ASPJ-1.1.0...
[==================================================================] 34/34 100%
bt Desktop #
```

3) recharger le module RT73

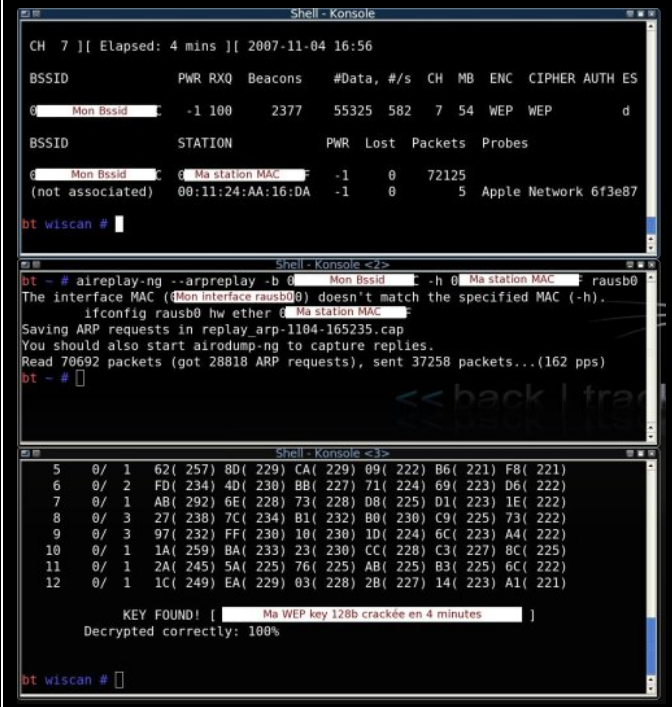
```
- rmmod rt73
- modprobe rt73
```

4) Activation du dongle

```
ifconfig rausb0 up
iwconfig rausb0 mode monitor
airmon-ng start rausb0
```

5) Exemple d'utilisation avec aircrack-ng

```
airodump-ng rausb0 -c 7 -b (mon bessid) -w (mon fichier cap)
aireplay-ng --arpreplay -b (mon bessid) -h (ma station mac) rausb0
aircrack-ng -z -b (mon bessid) (mon fichier cap).cap  --> seulement si aircrack-ng version 0.9 ou supérieur
aircrack-ng -a 1 -n 128 (mon fichier cap).cap
```



Problèmes

Channel Négatif

Nous pouvons rencontrer un bug sur aicrack qui implique un maintient sur un channel négatif (-1), pour cela il nous faut appliquer un patch de cette manière (adapter en fonction des versions/dates) :

```
#!/bin/bash
# Sanguinarius
# Patch aicrack for bypass negative channel (-1)
mkdir Airpatch
cd Airpatch
apt-get install linux-headers-$(uname -r)
wget http://wireless.kernel.org/download/compat-wireless-2.6/compat-wireless-2011-08-08.tar.bz2
tar -jxf compat-wireless-2011-08-08.tar.bz2
cd compat-wireless-2011-08-08
wget http://patches.aircrack-ng.org/channel-negative-one-maxim.patch
apt-get install patch
patch ./net/wireless/chan.c channel-negative-one-maxim.patch
make
make install
make unload
reboot
```

reverse cell phone lookup

reverse lookup

Dernière modification de cette page le 31 décembre 2011 à 03:57.
Cette page a été consultée 210 799 fois. Politique de confidentialité À propos de Backtrack-fr Avertissements
Powered By MediaWiki